Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (original): A method of signing a data string, comprising the steps of:

(a) hashing the data string and a seed value to generate a hash value;

(b) encoding into an image point the hash value, the seed value, and a given portion of the data string; and

(c) applying a given decryption primitive to the image point to obtain a digital signature of the data string.

2. (canceled)

3. (original): The method of digital signing as described in Claim 1 further including the step of concatenating the digital signature with a remaining portion of the data string to facilitate subsequent authentication.

4. (original): The method of digital signing as described in Claim 3 wherein the data string is recoverable from the given portion and the remaining portion.

5. (original): The method of digital signing as described in Claim 1 wherein the given portion of the data string is the data string.

6. (original): The method of digital signing as described in Claim 1 wherein the given portion of the data string is a null value.

Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

7. (currently amended): The method of digital signing as described in Claim 1 wherein the hash of the data string and the seed value in step 1(a) is computed by hashing a concatenation of the seed value and the data string.

8. (original): The method of digital signing as described in Claim 1 wherein the hash value, the seed value and the given portion of the data string are each recoverable given the image point.

9. (original): The method as described in Claim 1 wherein the given decryption primitive is the RSA decryption primitive.

10. (original): The method as described in Claim 1 wherein the seed value is selected from a group of seed values consisting essentially of a random value, a pseudorandom value, and a time-varying value.

11. (original): A computer-implemented method of signing and authenticating a data string M having a first portion M1 and a second portion M2, wherein the data string is recoverable from M1 and M2, comprising the steps of:

(a) hashing the data string and a random seed r to generate a hash value h(r,M);

(b) encoding into an image point y the hash value h(r,M), the random seed r, and the second portion M2 of the data string;

(c) applying a decryption primitive to the image point y to obtain a digital signature x of the data string; and

(d) associating the digital signature x with the first portion M1 of the data string.

12. (canceled)

Appl. No.: 09/879,849
Amdt. Dated: 06/15/2004
Off. Act. Dated: 01/15/2004

13. (currently amended): The computer-implemented method as described in Claim 11 wherein the digital signature is authenticated by:

(e) applying an encryption primitive to the digital signature x to generate a candidate image point;

(f) decoding the candidate image point to generate candidate values corresponding to the hash value h(r,M), the random seed r, and the second portion M2 of the data string;

(g) forming a candidate data string by combining the candidate value for the second part M2 of the data string with the first portion M1;

(h) verifying at least that the candidate value for the hash value h(r,M) equals the hash of (i) the candidate value for the random seed and (ii) the candidate data string; and

(i) accepting the candidate data string as the data string M if the verification in step 13(h) is positive.

14. (original): The computer-implemented method as described in Claim 11 wherein the data string is signed in a first computer and the digital signature is authenticated in a second computer.

15. (original): The computer-implemented method as described in Claim 11 wherein the decryption primitive is the RSA decryption primitive.

16. (original): The computer-implemented method as described in Claim 13 wherein the encryption primitive is the RSA encryption primitive.

17. (original): A method of authenticating a digital signature x of a data string M, wherein the digital signature x has been generated by applying a given decryption

primitive to an image point y, the image point y comprising a function of a seed value r, a hash value h(r,M), and a given portion of the data string, the method comprising the steps of:

(a) applying a given encryption primitive to the digital signature to generate a candidate image point;

(b) decoding the candidate image point to generate candidate values corresponding to the seed value r, the hash value h(r,M), and the given portion of the data string;

(c) forming a candidate data string by combining the candidate value for the given portion of the data string with other information;

(d) verifying at least that the candidate value for the hash value h(r,M) equals the hash of (i) the candidate value for the seed value and (ii) the candidate data string; and

(e) accepting the candidate data string as the data string M if the verification in step (d) is positive.

18. (original): A computer-implemented cryptographic system, comprising:

means for signing a data string M, the signing means comprising:

means for hashing a function of the data string and a seed value to generate a hash value;

means for encoding into an image point the hash value, the seed value, and a given portion of the data string; and

means, using a given primitive, for decrypting the image point to obtain a digital signature of the data string; and

means for authenticating the digital signature, the authenticating means comprising:

means, using a given primitive, for encrypting the digital signature to generate a candidate image point;

means for decoding the candidate image point to generate candidate values corresponding to the seed value, the hash value, and the given portion of the data string;

means for generating a candidate data string from at least the candidate value of the given portion of the data string;

means for verifying at least that the candidate value for the hash value corresponds to the hash of the candidate seed and the candidate data string; and

means responsive to the verifying means for accepting the candidate data string as the data string.

19. (original): A computer program product in a computer-readable medium for signing a data string M, comprising:

means for hashing the data string and a random seed value to generate a keyed hash value;

means for encoding into an image point the keyed hash value, the random seed value and a given portion of the data string; and

means, using a given primitive, for decrypting the image point to obtain a digital signature of the data string.

20. (original): The computer program product as described in Claim 19 wherein the given primitive is the RSA decryption primitive.

21. (original): The computer program product as described in Claim 19 wherein the given portion of the data string is the data string.

22. (canceled)

23. (previously presented): The computer program product as described in Claim 19 wherein the given function is an output of a generator applied to the keyed hash value.

24. (original): A computer-implemented method of signing a data string M having a first portion M1 and a second portion M2, wherein the data string is recoverable from M1 and M2, comprising the steps of:

(a) selecting a random seed r;

(b) hashing the data string and the random seed r to generate a hash value h(r,M);

(c) encoding into an image point y the hash value h(r,M), the random seed r, and the second portion M2 of the data string; and

(d) applying a decryption primitive to the image point y to obtain a digital signature x of the data string;

wherein the random seed r is selected so that the image string y is in the domain of the decryption primitive.

25. (currently amended): The method as described in Claim 24 further including the step of:

[[(d)]](e) concatenating the digital signature x with the first portion M1 of the data string.

Claims 26-27 (canceled)

28. (original): The method as described in Claim 24 wherein the decryption primitive is a Rabin decryption primitive.